Multispectral Imaging for Differential Face Morphing Attack Detection: A Preliminary Study

Raghavendra Ramachandra[†] Sushma Venkatesh[$] Naser Damer [*] Narayan Vetrekar[‡] R. S. Gad[‡]
[†] *Norwegian University of Science and Technology (NTNU), Gjøvik, Norway.*
[‡]*School of Physical and Applied Sciences, Goa University, Goa, India.*
[*]*Fraunhofer Institute for Computer Graphics Research, Germany.*
[$]*AiBA AS, Gjøvik, Norway.*
E-mail: {raghavendra.ramachandra}@ntnu.no

Abstract

Face morphing attack detection is emerging as an increasingly challenging problem owing to advancements in high-quality and realistic morphing attack generation. Reliable detection of morphing attacks is essential because these attacks are targeted for border control applications. This paper presents a multispectral framework for differential morphing-attack detection (D-MAD). The D-MAD methods are based on using two facial images that are captured from the ePassport (also called the reference image) and the trusted device (for example, Automatic Border Control (ABC) gates) to detect whether the face image presented in ePassport is morphed. The proposed multispectral D-MAD framework introduce a multispectral image captured as a trusted capture to acquire seven different spectral bands to detect morphing attacks. Extensive experiments were conducted on the newly created Multispectral Morphed Datasets (MSMD) with 143 unique data subjects that were captured using both visible and multispectral cameras in multiple sessions. The results indicate the superior performance of the proposed multispectral framework compared to visible images.

1. Introduction

Face Recognition Systems (FRS) are widely deployed in numerous real-life access control applications. Face biometrics are extensively used in border control scenarios, resulting in more than one billion electric passports (or ePassports) [5] in which the face is used as the primary identifier. The exponential growth in the adaptation of ePassports and automatic Border Control (ABC) gates has also increased the risk of attacking these systems. Among the different types of attacks on ePassports, morphing attacks have emerged as potential attacks by deceiving both humans (at passport applications and border control) and ABC gates [11, 29].

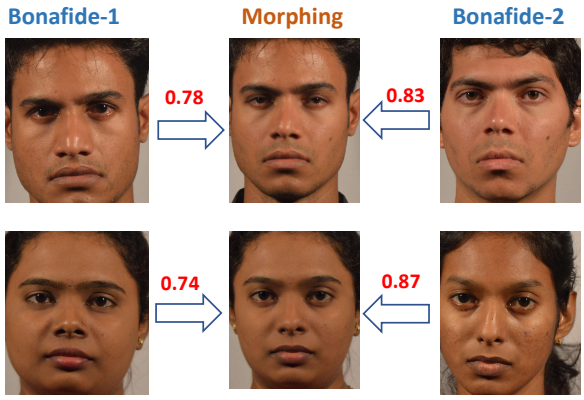

Figure 1. Example of face morphing images together with bona fide face images used for morphing. Comparison scores (higher is the better match) computed using Arcface FRS at FAR = 0.1% is also illustrated.

Morphing is defined as the process of seamlessly combining two or more face images from subjects such that the resulting morphing image indicates visual similarity to the source face images used for morphing. Extensive experiments reported in the literature [11, 15] show the vulnerability of FRS and the limitations of trained border guards in detecting morphed images. The attacker can use the morphing technique to generate the face images by blending his face image with the other data subject (also known as contributory data subjects) face image. The generated morphing image can then be used to obtain ID documents (e.g., ePassports) that can be used by all contributory data subjects. Morphing images can be generated using either landmark-based [10] or deep learning based [31] techniques. Further-

more, several open-source tools [29] enable attackers to easily generate morphing attacks. Figure 1 shows the example of morphing images together with the bona fide images that are used to generate the morphing images. Therefore, reliable detection of the face morphing image is necessary to achieve reliable user verification using the FRS.

Morphing Attack Detection (MAD) has been extensively studied in the literature, resulting in two types: single-image MAD (S-MAD)-based and differential-based MAD (D-MAD). S-MAD techniques are based on a single image to detect whether the presented face image is a bona fide or morph. The D-MAD methods are based on two images such that it uses the first image as the reference and then compares the given image with the reference image to detect the morphing attack. D-MAD techniques are well suited for the ABC scenario, where reference images can be taken from the passport and live captured images can be taken from the ABC gates. Various techniques are proposed for S-MAD, and D-MAD approaches [29]. The existing S-MAD approaches include texture features [19], hybrid texture features [21], Residual noise [6,30], deep features [16], multimodal features [22], and attention models [1]. The existing D-MAD approaches include de-morphing [2, 9], texture features [14], residual features [23], 3D information [25], deep learning [4, 18, 27, 28], legacy [3] and deep features [17, 20, 24]. For more details on the existing techniques for MAD readers, please refer to survey article [29]. Furthermore, it is worth noting that D-MAD techniques have demonstrated better detection accuracy compared to S-MAD techniques.

Existing studies on S-MAD and D-MAD have been developed based on the visible face image, in which the face images are captured with conventional cameras. However, the evolving technology for developing ABC gates is equipped with multispectral cameras [8]. This motivated us to consider multi-spectral imaging as the source of image capture, especially in the D-MAD setup. Multispectral imaging captures multiple images in different spectral bands that are complementary to each other. Hence, it is our assertion that the fusion of complementary spectral bands improves the detection performance of D-MAD techniques. In this work, we present a novel framework for D-MAD in which the reference images are captured from visible imaging and the live image is captured using multispectral imaging. More particularly, we introduce the following critical questions:

- **Q1:** Which spectral band indicates the highest morphing detection accuracy?
- **Q2:** Does the individual multispectral imaging improves the morphing attack detection compared to the visible imaging alone?
- **Q3:** Does the fusion of spectral bands improve the morphing attack detection compared to the visible imaging alone?

While answering the above research questions, the following are the main contributions of this work:

- To the best of our knowledge, this is the first study to address morphing attacks using multispectral imaging in the D-MAD framework.
- The new multispectral dataset comprised 143 unique data subjects, of which 86 corresponded to male and 57 corresponded to female data subjects. Furthermore, a visible image dataset corresponding to 143 unique subjects was also collected in two different sessions. The database is publicly available for research purposes (https://sites.google.com/view/narayanvetrekar/database/spectral-face-gender).
- Benchmarking the performance of two different D-MAD techniques based on deep features [24] and hierarchical deep SLERP [26].
- Extensive experiments benchmarking morphing attack detection results with individual spectral bands and comparison with visible imaging.

The remainder of this paper is organized as follows: Section 2 discusses the proposed multispectral framework for the D-MAD, Section 3 discusses the newly collected dataset with multi-spectral and visible samples, Section 4 discusses the experimental results, and finally, Section 5 draws conclusions and future work.

2. Multi-spectral Differential Morphing Attack Detection (D-MAD) Framework

In this section, we present the proposed multispectral D-MAD framework for reliable morphing attack detection. We assert that the use of multispectral images will provide complementary information, as it can capture multiple images corresponding to different spectral bands. Furthermore, each of these spectral images reflects different levels of identity information because of the skin reflectance of different spectral bands. Thus, the use of multispectral imaging will enhance both the complementary and identity information of the data subject, which can result in the accurate detection of morphing attacks.

Figure 2 shows the block diagram of the proposed multispectral framework for Differential morphing attack detection (D-MAD). The D-MAD approach is based on two images: the first is the reference image and the second is the image captured from the trusted device. Therefore, the D-MAD scenario is highly applicable for ABC gate border control applications where the reference image can be read from the epassport and the trusted (or live capture) can be obtained from the ABC gate cameras. The enrolment image from passports is from the visible spectrum. Because the applicant submits the passport application together with the passport photo, which is then re-digitized (scanned) to be stored in the passport. The trusted captured images in

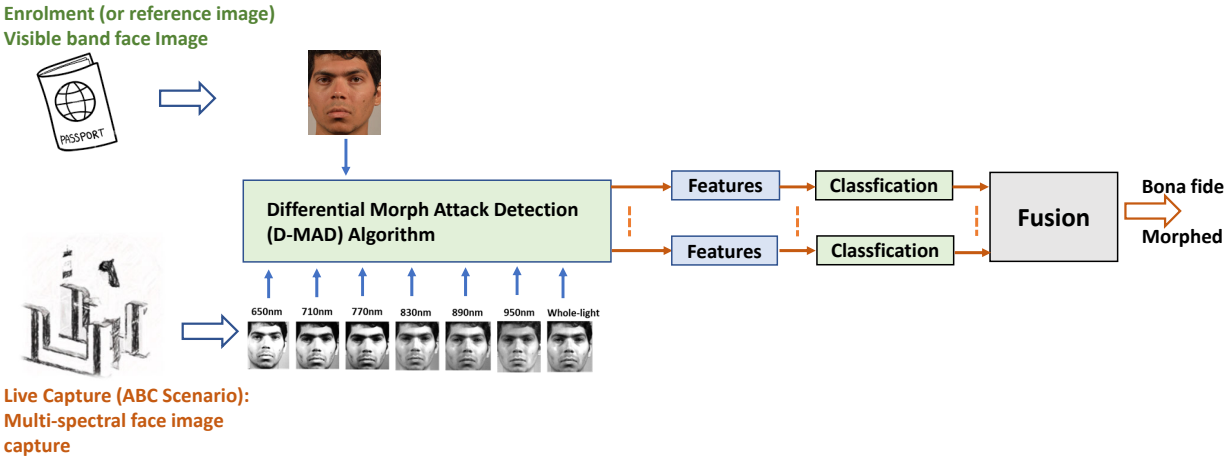

Figure 2. Block diagram of the proposed multispectral D-MAD framework

the proposed framework are from a multispectral camera that can render the images in the distinct spectral bands that complement each other. Each spectral image was used together with the reference image independently to extract the features that were classified to obtain the scores that were combined to make the final decision. The proposed framework can be structured into four functional units: (a) data capture, (b) D-MAD features, (c) classification scores and (d) fusion, as discussed below.

2.1. Data capture

The enrolment images were captured using a DSLR camera (Nikon D320) in a photo studio set up with uniform lighting. The captured image was further processed to achieve compatibility with ICAO-9303 [12] standards. Trusted device (or live) images were captured using a multispectral camera with a spatial resolution of 1.3Mpixels. In this work, we used six different spectral images captured at 650 nm, 710 nm, 770 nm, 830 nm, 890 nm, and 950 nm. Furthermore, we also captured a WholeLight (WL) image, which represents an image with no specific spectral filter. Let the reference image be R and the multispectral trusted captured images be $T_1, \ldots, T_N$, where $N = 1, 2, \ldots, 7$ corresponds to the spectral bands 650 nm, 710 nm, 770 nm, 830 nm, 890 nm, 950 nm and WL. More details on the data capture is discussed in the Section 3.

2.2. D-MAD features

The proposed framework can be used with existing D-MAD techniques because pairwise image processing is performed independently for individual spectral bands. Hence, in this study, we employed two D-MAD techniques to benchmark the performance of the proposed multispectral framework. The first D-MAD algorithm was based on deep features [24] that are based on the Arcface features [7]. Given the reference image R and the live image T_N, the deep features method extracts the face-related features using Arcface FRS on both R and T_N and provides difference features as the output. The second D-MAD method employed in this study is based on Hierarchical Deep Residual SLERP [26], which is based on six different pre-trained deep CNN networks. Furthermore, the feature differences between R and T_N were computed and combined using Spherical Linear Interpolation (SLERP) to output the final features. In this study, we selected these two D-MAD techniques by considering their performance and generalizability in detecting morphing attacks. The deep features [24] method also indicated good performance on the NIST benchmark, while Deep Residual SLERP [26] indicated superior performance over other existing methods, especially in the unconstrained border control scenarios.

2.3. Classification scores

The features computed from the individual D-MAD method corresponding to the individual spectral bands are then provided to the trained classifier to obtain the corresponding matching score. Because there are seven different spectral bands, we obtain seven different scores, $S_1, S_2, S_3, S_4, S_5, S_6, S_7$ corresponding to each feature. We used the same classifiers that were used with the existing D-MAD techniques employed in this study.

2.4. Fusion

Finally, the proposed framework combines the scores obtained in the previous step using the sum rule. Thus, the fused scores $F = \sum_{k=1}^{7} S_k$ is compared with the pre-set

threshold to make the final decision on the morphing detection.

3. Multispectral Morphing Dataset (MSMD)

This section presents a newly collected Multispectral Morphing dataset (MSMD). The MSMD dataset comprised 143 subjects (86 males and 57 females) with varying age groups from 22 to 72 years. The MSMD dataset was collected in multiple sessions to capture visible and multispectral images from 143 subjects.

3.1. Visible data collection:

The visible images are collected using DSLR camera (Model: Nikon D320) under constrained conditions. Because visible images represent passport images, special attention is required to achieve high-quality face image capture. Visible images were captured using a photo booth with uniform lighting, neutral pose, and expression. Visible data were captured in two sessions with a time gap of 30-45 days. Sesison-1 was collected under highly constrained conditions, while session-2 was collected under similar conditions. Session-1 is used as the enrolment samples and session-2 samples are used as the trusted capture in the experiments. In session-1, 13 images were captured and in session-2, 30 image samples were captured. Thus, the visible dataset comprised 143 subjects $\times$ 13 samples = 1859 samples in session-1 and 143 subjects $\times$ 30 samples = 4290 samples in session-2. Figure 3 shows the example visible images from session-1 and session-2 from the MSMD dataset.

3.2. Multispectral data collection:

The multispectral data were collected using a custom device built using a CMOS camera (Model: BCi5-U-M-40-LP) with 1.3 Mega pixels spatial resolution. In this study, we selected six different spectral bands, 650 nm, 710 nm, 770 nm, 830 nm, 890 nm, and 950 nm, together with the WholeLight (WL) image. We selected these six spectral bands to cover both visible (VIS) and near-infrared (NIR) wavelengths. Furthermore, the availability of the WholeLight image, in which the image is captured without any filters, represents the standard image captured with the VIS-NIR-sensitive camera. The dataset is collected in the indoor setting with two illumination units of a quartz tungsten halogen (QTH) light source. We have collected 11 samples for each data subject that will result in 143 subjects $\times$ 7 spectral bands $\times$ 11 = 11,011 samples. Figure 3 shows the example multispectral images from the MSMD dataset.

3.3. Morphing images:

The morphing images were generated using the visible images collected in session-1 of the visible image dataset. We selected one image per data subject and employed two morphing generation methods to create morphing attack samples. The first morphing generation is based on using landmarks [10] in which pixel-level information from the contributing data subjects is employed by wrapping and blending to generate high-quality morph images. The second morphing generation is based on a generative method called MIPGAN-2 [31], which uses GAN-2 as the backbone. The motivations behind the selection of these methods include (a) high-quality morphing image generation, (b) indicating high vulnerability with FRS [31] and (c) challenges to be detected using MAD techniques. [31].

To ensure a disjoint-morphing dataset, the dataset of 143 unique subjects was divided into two disjoint sets. The training set consisted of 78 data subjects and the testing set consisted of 65 datasets. Morphing is performed internally on the training and testing sets to achieve a complete disjoint set. In total, we had 1400 morphing images, of which the training set consisted of 928 images and the testing set consisted of 472 morphing images. Figure 4 shows an example of morphing the images from the MSMD dataset. Table 1 lists the statistics of the MSMD dataset, which is available to the semi-public for research purposes.

Table 1. Statistics of MSMD dataset summarising the data partition for training and testing set

Data Type	Training Set	Testing Set
Visible Images	1859	4290
Multispectral images	5698	5313
Morphing Images	928 $\times$2	472 $\times$2

4. Experiments and Results

In this section, we present quantitative results of the proposed multispectral D-MAD framework. The quantitative performance of the D-MAD techniques is presented using the ISO/IEC 30107 metrics [13] namely the "Attack Presentation Classification Error Rate (APCER (%)), which defines the proportion of attack images (face morphing images) incorrectly classified as bona fide images and the Bona fide Presentation Classification Error Rate (BPCER (%)) in which bona fide images incorrectly classified as attack images are counted [13] along with the Detection Equal Error Rate (D-EER (%))" [31].

4.1. Experimental protocols

We independently performed two experiments on the visible and multispectral data to benchmark the comparative performance of the D-MAD techniques employed in

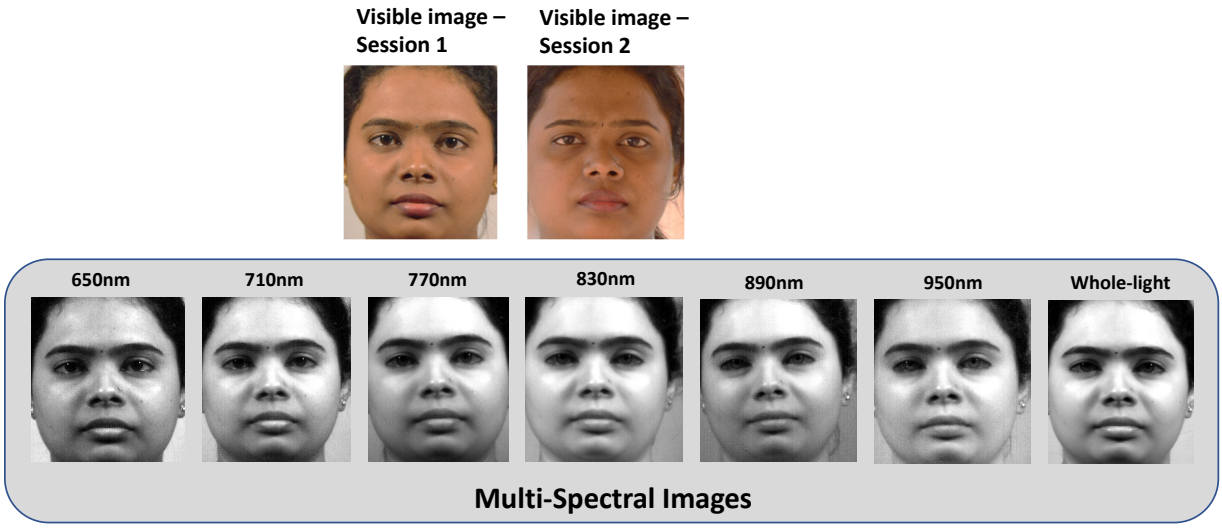

Figure 3. Example of visible (from session-1 and session-2) and multispectral images from MSMD dataset

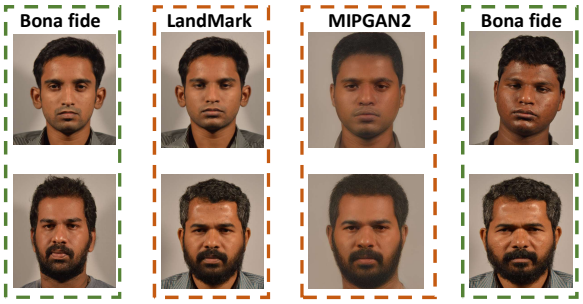

Figure 4. Example of face morphing images generated using Landmark and MIPGAN2 based morphing techniques.

this study. **Visible D-MAD experiments:** In this experiment, session-1 visible images represent the bona fide samples, and the corresponding morphed images as the morphing samples are used as the enrolment (or reference) image. The trusted capture device image is represented by the visible data captured in session-2. **Multispectral D-MAD experiments:** In this experiment, the reference images corresponding to bona fide and morphing samples were taken from the visible images collected in session-1. Trusted capture images were obtained from the multispectral data.

4.2. Results and Discussion

First, we present the results of the D-MAD algorithms for the individual spectral bands of the multispectral data. Table 2 shows the quantitative detection performance of the D-MAD techniques on two different types of morphing generation methods. Figure 5 and 6 show bar charts of the D-EER (%) corresponding to the individual spectral bands. For simplicity, we included bar charts for the landmark-based morphing generation method. Based on the obtained results, the following observations were made:

- The detection performance of the D-MAD techniques varies across different spectral bands. The variation in the detection performance was noted for both D-MAD techniques evaluated in this work.
- The detection performance is also influenced by the morphing generation technique used to generate morphing. The experimental results indicate that MIPGAN-based morphing images are easier to detect than landmark-based morphing methods. This observation is consistent with both visible and multispectral imaging.
- Among different spectral bands, the visible range bands (650nm and 710nm) indicates the lowest D-EER (%) with both D-MAD techniques. The improved performance can be attributed to the fact that both enrolment and trusted images are from the visible spectrum, and facial images possess rich texture information that can aid the detection process. This observation is consistent with both visible and multispectral imaging.
- The detection performance of D-MAD in the near-infrared spectral bands (830 nm, 890 nm, and 950 nm) indicates a slightly higher D-EER (%) compared to the visible spectral bands with landmark-based morphing.

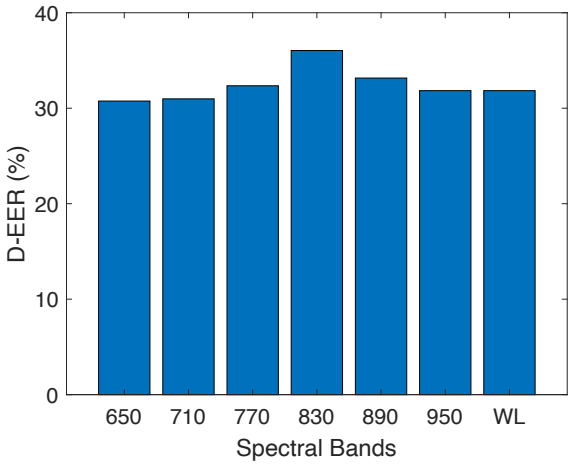

Figure 5. D-EER(%) performance of Deep features [24] on individual spectral bands: Landmark based morphing [10]

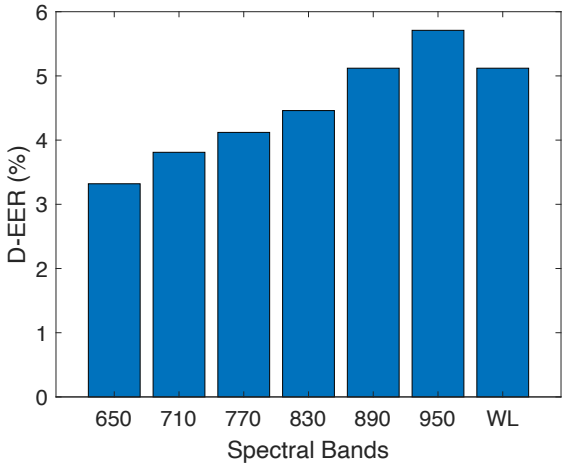

Figure 6. D-EER(%) performance of Hierarchical deep Residual SLERP [26] on individual spectral bands: Landmark based morphing [10]

Table 2. Quantitative detection performance of the D-MAD algorithms on individual spectral bands

Morphing Type	MAD Algorithms	Spectral Bands	D-EER (%)	BPCER @APCER = 5%	BPCER @APCER = 10%
Land Mark based Morphing [10]	Deep Features [24]	650	30.75	85.82	69.33
		710	30.98	87.18	71.19
		770	32.35	84.68	70.14
		830	36.14	89.66	84.3
		890	33.13	84.33	72.16
		950	31.84	85.67	69.85
		WL	29.61	84.71	68.81
	Hierarchical Deep Residual SLERP [26]	650	3.32	1.69	0.49
		710	3.81	2.98	1.22
		770	4.22	2.71	1.66
		830	4.46	3.74	1.14
		890	4.99	4.98	2.63
		950	5.5	5.74	3.34
		WL	5.12	5.2	2.63
MIPGAN-2 based Morphing [31]	Deep Features [24]	650	8.77	18.56	6.72
		710	9.41	23.97	8.55
		770	11.17	29.81	13.19
		830	11.73	27.60	13.98
		890	12.68	28.93	17.25
		950	9.89	25.75	9.82
		WL	10.63	24.52	11.59
	Hierarchical Deep Residual SLERP [26]	650	**0**	**0**	**0**
		710	**0**	**0**	**0**
		770	**0**	**0**	**0**
		830	**0**	**0**	**0**
		890	**0**	**0**	**0**
		950	**0**	**0**	**0**
		WL	**0**	**0**	**0**

However, the variation in D-EER (%) was not consistent across the two D-MAD techniques employed in this study. The deep features method [24], which is based on facial features, exhibits less variation in detection performance, especially in the NIR bands. However, the Hierarchical Deep Residual SLERP [26], which is based on texture features, indicates smaller variation in the detection performance, especially in NIR spectral bands, compared to the deep features method [24]. The possible variation in the Hierarchi-

Table 3. Quantitative performance of D-MAD techniques on visible and multispectral data

Morphing Type	Data Type	MAD Algorithms	D-EER (%)	BPCER @APCER = 5%	BPCER @APCER = 10%
Land Mark based Morphing [10]	Visible	Deep Features [24]	32.69	83.61	69.58
		Hierarchical Deep Residual SLERP [26]	5.15	5.19	2.17
	Multispectral	Deep Features [24]	21.64	48.51	34.37
		Hierarchical Deep Residual SLERP [26]	2.51	1.51	0.34
MIPGAN-2 based Morphing [31]	Visible	Deep Features [24]	17.73	36.69	26.32
		Hierarchical Deep Residual SLERP [26]	3.91	3.01	1.33
	Multispectral	Deep Features [24]	3.88	2.92	0.87
		Hierarchical Deep Residual SLERP [26]	**0**	**0**	**0**

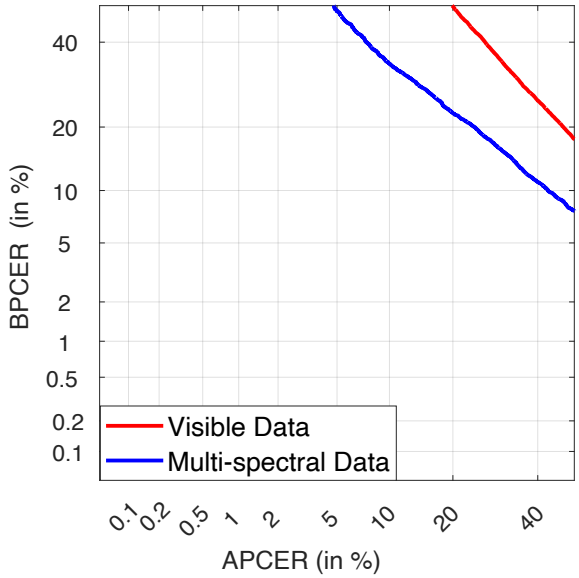

Figure 7. DET performance of Deep features [24] on visible and multispectral data: Landmark based morphing [10]

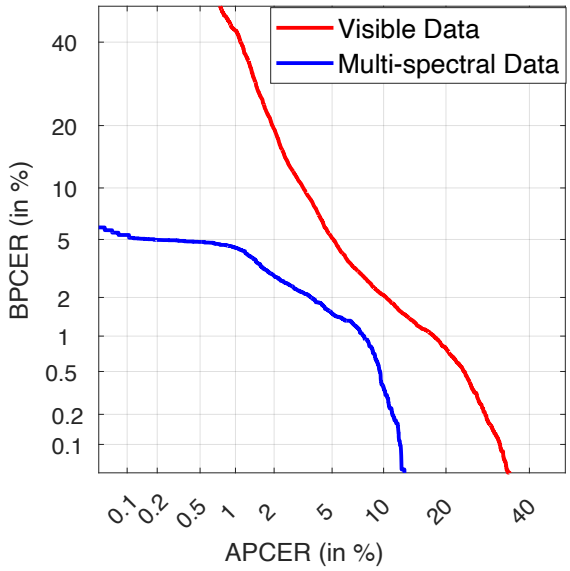

Figure 8. DET performance of Hierarchical Deep Residual SLERP [26] on visible and multispectral data: Landmark based morphing [10]

cal Deep Residual SLERP [26] can be attributed to the lack of texture information in the NIR spectral bands. Thus, the detection performance of D-MAD in the NIR spectrum depends on the type of D-MAD features used for morphing detection. The use of identity features (as in [24]) can indicate consistent performance across all spectral bands. However, the Hierarchical Deep Residual SLERP [26] D-MAD has indicated the better performance across all spectral bands compared to the deep features method [24].

- The use of wholeLight (WL) that is captured without any spectral filtering indicates the varied detection performance with respect to D-MAD techniques. The detection error with the deep features method [24] on WL images indicates a performance similar to that of both the VIS and NIR spectral bands. Because the deep features method [24] is based on facial features, it is less sensitive to different spectral bands, which may be due to the backbone model that is trained only using VIS images. However, the performance of Hierarchical Deep Residual SLERP [26] on WL images shows degraded performance compared to the VIS spectral bands.

Table 3 lists the performance of the D-MAD algorithms on the proposed multispectral framework and visible images. Both multispectral and visible data are collected using the same data subjects, and this can provide insights into the utility of multispectral images for reliable morphing attack detection. Furthermore, the performance of the multispectral framework was presented by fusing the results of all individual spectral bands. Figure 7 and 8 show the D-MAD technique DET curves for both the visible and multispectral data. The following are critical observations based on the results.

- In general, the performance of the D-MAD algorithms indicates a superior detection accuracy on the multispectral data compared to the visible data. This can be attributed to the fusion of complementary spectral bands, which can contribute to a higher detection accuracy. Improved detection performance can be noticed with both D-MAD techniques on multispectral data.
- The D-MAD method based on the Hierarchical Deep Residual SLERP [26] indicates the superior performance on visible and multispectral data.
- Landmark-based morphing is more challenging to detect than MIPGAN-based morphing techniques. However, the proposed multispectral approach indicated higher detection accuracy for both morphing types. These results justify the efficacy of the proposed multispectral approach for face morphing detection.

4.3. Discussion

Based on the observations from the above experiments and obtained results, the research questions formulated in Section 1 are answered below.

- **Q1**. Which spectral band indicates the highest morphing detection accuracy?
  - Based on the experimental results reported in Table 2, the visible spectral bands indicate better detection accuracy on the textures-based D-MAD [26]. However, the performance across the spectral bands is comparable when D-MAD with facial features [24] is used. The performance of the D-MAD techniques varies with the type of morphing generation technique. The multispectral D-MAD approach when morphing generation is MIPGAN, indicates good detection performance across all spectral bands.
- **Q2**. Does the individual multispectral imaging improves the morphing attack detection compared to the visible imaging alone?
  - Based on the quantitative performance reported in Tables 3 and 2, the individual spectral bands indicate slightly better performance compared to the visible images alone. Improved performance of the individual spectral bands can be observed with both D-MAD techniques. However, with MIPGAN-based morphing, individual spectral bands indicate higher detection accuracy than the visible band alone with D-MAD approaches.
- **Q3:** Does the fusion of spectral bands improves the morphing attack detection compared to the visible imaging alone?
  - Based on the quantitative performance reported in Table 3, multispectral images indicate the highest detection accuracy compared to visible images. The improved performance is confirmed with two different D-MAD algorithms that are based on facial features [24] and textures features [26]. Hence, irrespective of the type of features used by the D-MAD techniques, the proposed multispectral framework indicated improved morphing-detection accuracy with different types of morphing-generation methods.

5. Conclusion

In this paper, we presented a multispectral framework for differential morphing attack detection. The D-MAD framework utilizes two images. The first image is taken from ePassport (a.k.a reference image), and the second image is taken from the trusted capture (e.g., ABC gates) to detect the morphing attack on ePassport. The proposed framework captures seven different spectral bands as the trusted capture, which is further used with the reference image from the visible spectrum to reliably detect morphing attacks on ePassport. In this study, two different D-MAD techniques based on facial and texture features are employed within the proposed multispectral framework to compare the morphing detection performance of the multispectral approach with visible images. Extensive experiments were conducted on a newly built dataset with 143 unique data subjects. The obtained results demonstrate the superior performance of the proposed multispectral D-MAD compared to visible images on two different types of morphing generation techniques . Future work will extend the present work (a) with different print and scan sources for morphing image generation and (2) with different light sources for multispectral image capture.

References

[1] P. Aghdaie, B. Chaudhary, S. Soleymani, J. Dawson, and N.M. Nasrabadi. Attention aware wavelet-based detection of morphed face images. In *2021 IEEE International Joint Conference on Biometrics (IJCB)*, pages 1–8, 2021. 2

[2] S. Banerjee and A. Ross. Conditional identity disentanglement for differential face morph detection. In *2021 IEEE International Joint Conference on Biometrics (IJCB)*, pages 1–8, 2021. 2

[3] Ilias Batskos, Florens F de Wit, Luuk J Spreeuwers, and Raymond J Veldhuis. Preventing face morphing attacks by using legacy face images. *IET biometrics*, 10(4), 2021. 2

[4] G. Borghi, E. Pancisi, M. Ferrara, and D. Maltoni. A double siamese framework for differential morphing attack detection. *Sensors*, 21(10), 2021. 2

[5] Best Citizenship. e-Passport. https://best-citizenships.com/2021/02/12/epassports-used-by-over-1-billion-people-for-travels//. 1

[6] L. Debiasi, U. Scherhag, C. Rathgeb, A. Uhl, and C. Busch. PRNU variance analysis for morphed face image detection. In *Proc. of 9th Intl. Conf. on Biometrics: Theory, Applications and Systems (BTAS 2018)*, 2018. 2

[7] J. Deng, J. Guo, and S. Zafeiriou. ArcFace: Additive angular margin loss for deep face recognition. In *Conf. on Computer Vision and Pattern Recognition (CVPR)*, June 2019. 3

[8] MODI eGates. MODI eGates. http://gabena.hu/modi/doc/Kiosk_Eng.pdf. 2

[9] M. Ferrara, A. Franco, and D. Maltoni. Face demorphing in the presence of facial appearance variations. In *Proc. of the 26th European Signal Processing Conf. (EUSIPCO)*. IEEE, September 2018. 2

[10] M. Ferrara, A. Franco, and D. Maltoni. Decoupling texture blending and shape warping in face morphing. In *Intl. Conf. of the Biometrics Special Interest Group (BIOSIG)*. IEEE, September 2019. 1, 4, 6, 7

[11] Sankini Rancha Godage, Frøy Løvåsda, Sushma Venkatesh, Kiran Raja, Raghavendra Ramachandra, and Christoph Busch. Analyzing human observer ability in morphing attack detection–where do we stand? *arXiv preprint arXiv:2202.12426*, 2022. 1

[12] International Civil Aviation Organization. Machine readable passports – part 9 – deployment of biometric identification and electronic storage of data in eMRTDs. http://www.icao.int/publications/Documents/9303_p9_cons_en.pdf, 2015. 3

[13] ISO/IEC JTC1 SC37 Biometrics. *ISO/IEC 30107-3. Information Technology - Biometric presentation attack detection - Part 3: Testing and Reporting*. International Organization for Standardization, 2017. 4

[14] S. Lorenz, U. Scherhag, C. Rathgeb, and C. Busch. Morphing attack detection: A fusion approach. In *2021 IEEE 24th International Conference on Information Fusion (FUSION)*, pages 1–7, 2021. 2

[15] A. Makrushin, D. Siegel, and J. Dittmann. Simulation of border control in an ongoing web-based experiment for estimating morphing detection performance of humans. In *Proceedings of the 2020 ACM Workshop on Information Hiding and Multimedia Security*, IH&MMSec '20, page 91–96, New York, NY, USA, 2020. Association for Computing Machinery. 1

[16] Iurii Medvedev, Farhad Shadmand, and Nuno Gonçalves. Mordeephy: Face morphing detection via fused classification. *arXiv preprint arXiv:2208.03110*, 2022. 2

[17] D. Ortega-Delcampo, C. Conde, D. Palacios-Alonso, and E. Cabello. Border control morphing attack detection with a convolutional neural network de-morphing approach. *IEEE Access*, 8:92301–92313, 2020. 2

[18] F. Peng, L. Zhang, and M. Long. FD-GAN: Face demorphing generative adversarial network for restoring accomplice's facial image. *IEEE Access*, June 2019. 2

[19] R. Raghavendra, K. Raja, and C. Busch. Detecting morphed face images. In *2016 IEEE 8th Intl. Conf. on Biometrics: Theory, Applications and Systems (BTAS)*. 8th IEEE Intl. Conf. on Biometrics: Theory, Applications and Systems (BTAS-2016), IEEE, September 2016. 2

[20] R. Raghavendra, K. Raja, S. Venkatesh, and C. Busch. Transferable deep-CNN features for detecting digital and print-scanned morphed face images. In *IEEE Conf. on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pages 1822–1830, 2017. 2

[21] R. Raghavendra, S. Venkatesh, K. Raja, and C. Busch. Towards making morphing attack detection robust using hybrid scale-space colour texture features. In *IEEE 5th Intl. Conf. on Identity, Security, and Behavior Analysis (ISBA)*. IEEE, January 2019. 2

[22] Raghavendra Ramachandra and Guoqiang Li. Multimodality for reliable single image based face morphing attack detection. *IEEE Access*, 10:82418–82433, 2022. 2

[23] Raghavendra Ramachandra and Guoqiang Li. Residual colour scale-space gradients for reference-based face morphing attack detection. In *2022 25th International Conference on Information Fusion (FUSION)*, pages 1–8. IEEE, 2022. 2

[24] U. Scherhag, C. Rathgeb, J. Merkle, and Christoph Busch. Deep face representations for differential morphing attack detection. *IEEE Trans. on Information Forensics and Security*, 2020. 2, 3, 6, 7, 8

[25] J. Singh, K. Raja, R. Raghavendra, and C. Busch. Robust morph-detection at automated border control gate using deep decomposed 3D shape & diffuse reflectance. In *Proc. of the 15th Intl. Conf. on Signal Image Technology & Internet Based Systems (SITIS)*, November 2019. 2

[26] Jag Mohan Singh and Raghavendra Ramachandra. Reliable face morphing attack detection in on-the-fly border control scenario with variation in image resolution and capture distance. In *2022 IEEE International Joint Conference on Biometrics (IJCB)*, pages 1–10. IEEE, 2022. 2, 3, 6, 7, 8

[27] S. Soleymani, B. Chaudhary, A. Dabouei, J. Dawson, and N. Nasrabadi. Differential morphed face detection using deep siamese networks. In *International Conference on Pattern Recognition*, pages 560–572. Springer, 2021. 2

[28] S. Soleymani, A. Dabouei, F. Taherkhani, J. Dawson, and N. Nasrabadi. Mutual information maximization on disentangled representations for differential morph detection. In *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision (WACV)*, pages 1731–1741, January 2021. 2

[29] S. Venkatesh, R. Raghavendra, K. Raja, and C. Busch. Face morphing attack generation and detection: A comprehensive survey. *IEEE Transactions on Technology and Society*, 2(3):128–145, March 2021. 1, 2

[30] S. Venkatesh, R. Raghavendra, K. Raja, L. Spreeuwers, R. Veldhuis, and C. Busch. Detecting morphed face attacks using residual noise from deep multi-scale context aggregation network. In *2020 IEEE Winter Conference on Applications of Computer Vision (WACV)*, pages 269–278. IEEE, March 2020. 2

[31] H. Zhang, S. Venkatesh, R. Raghavendra, K. Raja, N. Damer, and C. Busch. MIPGAN—Generating strong and high quality morphing attacks using identity prior driven GAN. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 3(3):365–383, 2021. 1, 4, 6, 7